GETS

Function is intrinsically unsafe and should not be used

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4908 bytes

Attack Category	• Malicious Input
Vulnerability Category	• Buffer Overflow • Input source (not really attack) • Unconditional
Software Context	• String Management
Location	
Description	The gets() function is intrinsically unsafe and should not be used. The gets() function reads characters from stdin and stores them in a buffer until a newline or EOF character is encountered. There is no way to specify the size of the buffer, and so this function is very vulnerable to buffer overflows.
APIs	**FunctionName** / **Comments** _getts _getws gets
Method of Attack	The gets() function is unsafe because it does no form of bounds checking on the input size. An attacker can feed arbitrarily sized inputs to gets() and easily overrun a buffer.
Exception Criteria	None. Do not use gets().
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** C code / Use an input function that has a limit on the number of characters that will be read into the buffer. / Eliminates the buffer overflow problem, but fgets() is deprecated because if there is a null in the input data it will be

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

		Replace gets() with fgets(buf, sizeof(buf), stdin) or a C++ stream object. If "buf" is a static buffer locally defined, add a sizeof(buf)-1 call. If malloc'd locally, use the malloc size (minus 1). Make sure there is a "\0" at the end of the buf when returning.	misinterpreted as an end of string terminator.
	C++ code	Replace gets() with a C++ stream method that has a limit on the number of characters that will be read into the buffer (cin.getline(buffer, bufSize), for example). If "buf" is a static buffer locally defined, bufSize can be replaced by sizeof(buffer). If malloc'd, use the malloc size.	Effective as long as buffer size is correctly specified.
Signature Details	The gets() function is called.		

Examples of Incorrect Code	`char str1[10];`
	`gets(str1);`
	`/* If the string is more than 10 characters, the overflow will spill over into the adjoining memory. */`		

Examples of Corrected Code	`char str1[10];`
	`fgets(str1, sizeof(str1), stdin);`
	`/* Will not overflow.`		

	Note that if buffer is malloc'd, sizeof() will not work and the malloc size should be used. */ /* In C++, use of iostream::getline() is preferred. */
Source References	• Viega, John & McGraw, Gary. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X , pg. 142. • Howard, Michael & LeBlanc, David C. *Writing Secure Code, 2nd ed*. Redmond, WA: Microsoft Press, 2002, ISBN: 0735617228.
Recommended Resources	
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com